The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
07/09/2013

SUBJECT:
Multiple Security Vulnerabilities reported in Google Chrome

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEM AFFECTED:
Google Chrome Prior to 28.0.1500.71

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Google Chrome. Details of these vulnerabilities are as follows:

A security vulnerability exists in Block pop-unders in various scenarios. [CVE-2013-2867]
A security vulnerability occurs due to confusion setting up sign-in and sync. [CVE-2013-2879]
A security vulnerability occurs due to the incorrect synchronization of the NPAPI extension component. [CVE-2013-2868]
An out-of-bounds-read condition exists when handling JPEG2000. [CVE-2013-2869]
A use-after-free vulnerability occurs when handling network sockets. [CVE-2013-2870]
A security-bypass vulnerability, which allows attackers to perform man-in-the-middle attacks against HTTP in SSL. [CVE-2013-2853]
A use-after-free vulnerability exists in input handling. [CVE-2013-2871]

A security vulnerability exists due to a possible lack of entropy in renderers. [CVE-2013-2872]
A use-after-free vulnerability exists in resource loading. [CVE-2013-2873]
An information disclosure vulnerability that allows screen data leak with GL textures. [CVE-2013-2874]
An out-of-bounds read condition exists in SVG. [CVE-2013-2875]
A security-bypass vulnerability due to Extensions permissions confusion with interstitials. [CVE-2013-2876]
An out-of-bounds read in XML parsing. [CVE-2013-2877]
A security vulnerability affects the 'viewsource' attribute on iframes.
An out-of-bounds read condition exists in text handling. [CVE-2013-2878]
Various fixes from internal audits, fuzzing and other initiatives (Chrome 28) [CVE-2013-2880]

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
Do not open email attachments or click on URLs from unknown or untrusted sources.

REFERENCES:

Google:

http://googlechromereleases.blogspot.com/2013/07/stable-channel-update.html

Security Focus:

http://www.securityfocus.com/bid/61041

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2853
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2867
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2868
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2869
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2870
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2871
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2872
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2873
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2874
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2875
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2876
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2877
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2878
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2879
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2880